§ 4 Die reellen Zahlen (Körperaxiome)

4.1 Definition Eine Menge K mit zwei Verknüpfungen

$$+ : K \times K \longrightarrow K, \quad (x,y) \mapsto x+y$$

$$\cdot : K \times K \longrightarrow K, \quad (x,y) \mapsto x \cdot y$$

heißt Körper (field), falls

(K1) K mindestens zwei Element enthält

(K2) $\forall\, x, y, z \in K$ gilt:

$(x+y)+z = x+(y+z)$, $(x \cdot y) \cdot z = x \cdot (y \cdot z)$ (Assoziativgesetze)

$x+y = y+x$ $\qquad x \cdot y = y \cdot x$ (Kommutativgesetze)

$x \cdot (y+z) = x \cdot y + x \cdot z$ (Distributivgesetz)

(K3) Es gibt Elemente $0, 1 \in K$ so, dass $\forall x \in K$ gilt:

(i) $x + 0 = x$

(ii) $x \cdot 1 = x$ (Existenz neutraler Elemente)

(iii) $\forall x \in K\ \exists\, x' \in K : x + x' = 0$

(iv) $\forall x \in K^* := K \setminus \{0\}\ \exists\, x^* \in K$ mit $x x^* = 1$ (Existenz der Inversen)

4.2 Beispiele (i) $(\mathbb{Q}, +, \cdot)$ ist ein Körper

(ii) $(\mathbb{R}, +, \cdot)$ ist ein Körper

(iii) $(\mathbb{Z}, +, \cdot)$ ist kein Körper, da für $x \in \mathbb{Z} \setminus \{\pm 1\}$ keine multiplikativen Inversen existieren.

(iv) Ist p eine Primzahl, so ist

$$\mathbb{F}_p := \mathbb{Z}/p = \{\bar{0}, \bar{1}, \ldots, \overline{p-1}\}$$

ein Körper bzgl. der Verknüpfungen

$$\bar{m} \pm \bar{n} = \overline{m \pm n}$$

Alle Axiome sind klar, bis auf die Existenz multiplikativer Inverser:

Sei $\overline{m} \in \mathbb{F}_p^*$

$\Rightarrow \quad ggT(m,p) = 1 \overset{3.10}{=} um + vp$ mit geeigneten $u, v \in \mathbb{Z}$

$\Rightarrow \quad \overline{1} = \overline{um} + \underbrace{\overline{vp}}_{=0} = \overline{um} = \overline{m}\,\overline{u}$

Man kann u (also auch $\overline{u}$) mit dem Euklidischen Algorithmus berechnen (3.10)

4.3 <u>Def.</u> Eine Menge $(R, +, \cdot)$ mit zwei Verknüpfungen, für die alle Axiome bis auf (K1) und (K3)(iv) gelten, heißt <u>kommutativer Ring mit Eins</u>

<u>Beispiele</u> (komm. Ringe mit Eins)

(i) $(\mathbb{Z}, +, \cdot)$

(ii) $(\mathbb{Z}/n, +, \cdot)$ für $n \in \mathbb{Z}_{>1}$

4.4 <u>Folgerungen aus den Körperaxiomen</u>

(a) Die Elemente 0 und 1 sind eindeutig bestimmt durch (K3)(i) bzw. (ii).

(b) zu jedem $x \in K$ existiert genau ein $x' \in K$ mit $x + x' = 0$.

(c) " $x \in K^*$ " $x^* \in K$ mit $x \cdot x^* = 1$.

(d) $\forall\ x, y, z \in K$ gilt $(x+y)z = xz + yz$

<u>Bew.</u>: (a) Sei auch $\tilde{0} \in K$ mit $x + \tilde{0} = x \quad \forall x \in K$

$\Rightarrow \tilde{0} \overset{K3}{=} \tilde{0} + 0 \overset{KG}{=} 0 + \tilde{0} = 0$. Eindeutigkeit von 1 genauso.

(b) Sei $x + x' = x + x'' = 0$

$\Rightarrow x' \overset{K3}{=} x' + 0 = x' + (x + x'') \overset{AG}{=} (x' + x) + x'' \overset{KG}{=} (x + x') + x''$

$= 0 + x'' \overset{KG}{=} x'' + 0 = x''$

(c) Genauso wie in (b).

(d) $(x+y)z \overset{KG}{=} z(x+y) \overset{DG}{=} zx + zy \overset{KG}{=} xz + yz$ ▨

<u>Schreibweisen</u> Für $x, y \in K$, $z \in K^*$ schreiben wir

$-x :=$ für das Element $x' \in K$ mit $x + x' = 0$, $x - y := x + (-y)$,

$z^{-1} :=$ für das Element $z^* \in K$ mit $zz^* = 1$, $\frac{x}{z} := xz^{-1}$.

<u>4.5 Satz</u> Sei K ein Körper

(a) Für $a, b \in K$ hat die Gleichung $a + x = b$ genau eine Lösung, nämlich $x = b - a$.

(b) Für $a \neq 0$ und $b \in K$ hat die Gleichg $ax = b$ genau ein Lösung, nämlich $x = a^{-1}b$.

(c) Für $a, b \in K$ gilt: $ab = 0 \Leftrightarrow a = 0$ oder $b = 0$

(d) $-0 = 0$, $1 \neq 0$, $1^{-1} = 1$

Für $x, y \in K$, $z, w \in K^*$ gilt

(e) $-(-x) = x$, $(z^{-1})^{-1} = z$

(f) $-(x+y) = -x - y$, $(zw)^{-1} = w^{-1}z^{-1}$

(g) $(-x)y = -(xy) = x(-y)$, $(-x)(-y) = xy$

<u>Beweis</u>: (a) Seien $a, b \in K$. Wegen

$$a + (b - a) = a + (b + (-a)) \overset{KG}{=} a + ((-a) + b) \overset{AG}{=} (a + (-a)) + b = 0 + b \overset{KG}{=} b$$

hat die Gleichung $a + x = b$ eine Lösung. Ist x eine Lösung, so gilt

$$x = ((-a) + a) + x \overset{AG}{=} (-a) + (a + x) = (-a) + b \overset{KG}{=} b + (-a) = b - a.$$

(b) Genauso wie (a).

(c) Seien $a, b \in K$

$$\Rightarrow a \cdot 0 = a \cdot (0 + 0) = a \cdot 0 + a \cdot 0 \Rightarrow 0 \cdot a = a \cdot 0 = 0$$

Sei $ab = 0$. Falls $a \neq 0$ ist, folgt

$$b = (a^{-1}a)b = a^{-1}(ab) = a^{-1} \cdot 0 = 0.$$

(d) $0 + 0 = 0 \Rightarrow -0 = 0$

$1 \neq 0$, denn sonst: $x = x \cdot 1 = x \cdot 0 = 0 \quad \forall x \in K$ ↯ zu (K1)

$1 \cdot 1 = 1 \Rightarrow 1^{-1} = 1$

(e) $(-x) + x \overset{KG}{=} x + (-x) = 0 \Rightarrow x = -(-x)$

$(z^{-1})z \overset{KG}{=} z(z^{-1}) = 1 \Rightarrow z = (z^{-1})^{-1}$

(f) $(x+y) + (-x-y) \overset{KG}{=} (x+y)(-y-x) \overset{AG}{=} x + (y + (-y-x)) \overset{AG}{=} x + ((y + (-y)) + x)$

$= x + (0 - x) = x - x = 0 \Rightarrow -(x+y) = -x-y$

2. Teil genauso.

(g) $xy + (-x)y \overset{DG}{=} (x - x)y = 0y = 0 \Rightarrow (-x)y = -(xy) \overset{\text{genauso}}{=} x(-y)$

$(-x)(-y) = -(x(-y)) \overset{KG}{=} -((-y)x) = -(-(yx)) \overset{(e)}{=} yx = xy$ ☒

<u>Folgerung</u> Ist $n \in \mathbb{Z}_{>1}$ keine Primzahl, d.h.

$$n = rs \quad \text{mit} \quad 1 < r, s < n,$$

so ist $\bar{r}\bar{s} = \bar{n} = 0$ in $\mathbb{Z}/_n$, aber $\bar{r} \neq 0 \neq \bar{s}$.
Also ist $\mathbb{Z}/_n$ kein Körper.